

CITY OF SUNNYVALE

The Heart of Silicon Valley

456 WEST OLIVE AVENUE

SUNNYVALE, CALIFORNIA 94086

(408) 730-7470

February 22, 2005

Dean J. Chu
Mayor

Ron Swegles
Vice Mayor

Frederik M. Fowler
Councilmember

Melinda Hamilton
Councilmember

John N. Howe
Councilmember

Otto Lee
Councilmember

Julia E. Miller
Councilmember

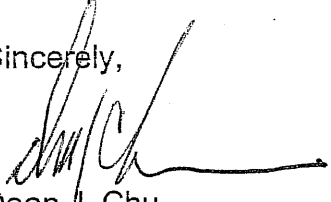
Mr. Dennis Hickey and Ms. Darlene Thorne
Santa Clara County Civil Grand Jury
191 North First Street
San Jose, CA 95113

Dear Mr. Hickey and Ms. Thorne:

The City of Sunnyvale received your letter dated January 27, 2005 requesting a status of the City's actions taken in response to the Findings and Recommendations of the 2002-2003 Santa Clara County Civil Grand Jury.

Enclosed is a copy of the Draft Disaster Recovery Plan developed by the City of Sunnyvale. The Plan covers both mission critical and non-critical information systems. The Plan is still in draft format and, therefore, has not been formally tested although system recovery is one of the Information Technology Department's routine operational tasks. The City will test the Plan as resources are available and finalize the Plan as appropriate.

Sincerely,



Dean J. Chu
Mayor

Enclosure

cc: Amy Chan, City Manager
Shawn Hernandez, Director of Information Technology
Don Johnson, Chief of Public Safety

City of Sunnyvale
D R A F T
Disaster Recovery Plan

Table of Contents

TABLE OF CONTENTS	2
MISSION.....	
DISASTER DEFINITION	
PLAN ADMINISTRATION	
PLAN EXERCISE.....	
PLAN STRUCTURE.....	
RECOVERY PROCESS OVERVIEW.....	
OPERATING PRINCIPLE.....	
RECOVERY ORGANIZATION & AUTHORITY.....	
DISASTER DECLARATION	
PLAN ACTIVATION	
EVENT LOGGING	
CITY INFORMATION.....	
NETWORK, SERVER AND APPLICATION RECOVERY LIST	
SERVER BACKUP AND RECOVERY PROCEDURES.....	
SERVER BACKUP PROCEDURES	
SERVER RECOVERY PROCEDURES.....	
NETWORK BACKUP AND RECOVERY PROCEDURES.....	
NETWORK BACKUP PROCEDURES	
NETWORK RECOVERY PROCEDURES	
MUNICIPAL AND ACCOUNTING SERVICES RECOVERY	
PRIMARY RECOVERY TEAM ASSIGNMENTS.....	
RECOVERY MANAGER.....	
RECOVERY MANAGER ASSIGNMENTS.....	
OPERATIONS RECOVERY TEAM.....	
OPERATIONS TEAM ASSIGNMENTS.....	
PUBLIC SAFETY SERVICES RECOVERY ASSIGNMENTS	
APPENDICES A.....	
DISASTER RECOVERY EVENT AND DISBURSEMENT LOG	
EVENT LOG	
APPENDICES B.....	
CONTACT LIST	

NETWORK AND SERVER CONTACTS

SERVER LISTING

APPLICATION LISTING.....

MISSION

The mission of this Disaster Preparedness Plan (DPP) is to provide an affordable, maintainable, and workable plan to assist in the recovery of processing in the City of Sunnyvale Annex and DPS Computer Operations Centers. This plan is designed to protect the City's Computer Operations Centers from the most probable short-term disasters.

The primary assumption is that this disaster preparedness document only covers a short-term disaster outage that is directly related to Finance: Accounting Services and Municipal Services. This document represents a recovery scenario of two business days or less of system unavailability.

Typical Emergency Situation

Duration of Recovery

Disk Failure, System Failure, Gateway Failure	Outage is 0 to 2 business days
---	--------------------------------

The following areas are not addressed as part of this plan: telecommunications (voice), network environment (data), vital paper or paper image documents, and microfilm.

Disaster Definition

A disaster is defined as any situation that causes an inability to process beyond the time period necessary to resume operation of critical applications. A disaster can be anything from a fire, disk drive crash, power outage to a catastrophic disaster like an earthquake, explosion or flood. Typically the first line of defense in disaster planning is to have appropriate documentation in place that clearly identifies all hardware, software, applications, data communications, network systems, configurations and a recovery plan for those components.

There are two phases to disaster recovery planning, short-term disaster preparedness and long-term disaster recovery. Both planning efforts require analysis, establishing procedures, collecting environmental information and documentation of appropriate recovery processes and procedures.

This planning effort documents short-term disaster preparedness and is primarily designed around the backup and recovery of systems and data, versus the loss of the entire Computer Operations Centers. The following is an outline of those components include in the short-term disaster preparedness plan.

Short-Term Disaster Preparedness

Emergency Management Plan

Define disaster definition

Plan scope

Determine plan administration and structure

Notification Procedures

Recovery Team Assignments

Escalation procedures

Notification process

Contact lists – Computer Services, City staff

Vendor list

Backup Procedures

Backup procedures in place for all systems

Off site tape recovery

Retention management procedures

Event logging

Recovery Procedures

Recovery procedures for all systems

Off site recovery procedures to return appropriate tapes and documentation

Testing the Disaster Plan

Emulate disaster scenario

Test all procedures

Evaluate and report test results

System verification, startup and test

On-Going Control and Maintenance

Modify the plan to accommodate changes to hardware and software

Update information on critical production and PC applications

Maintain inventory of equipment and configurations

Evaluate effectiveness of the recovery process, including testing and recommend/make changes as appropriate.

Plan Administration

This Disaster Preparedness Plan (DPP) shall be maintained and administered by the Director of Information Technology, Shawn Hernandez. Each section of the Disaster Preparedness Binder shall be reviewed and updated annually.

Plan Exercise

This Disaster Preparedness Plan should be exercised annually to test its effectiveness and updated for changing conditions and requirements. Only through periodic exercise can there be confidence the Plan will operate as documented under actual disaster conditions.

The exercises should be conducted using varying disaster scenarios and pre-defined scripts that test the ability of the recovery team to respond effectively to a disaster situation. Typically, a recovery team and disaster plan are not fully "shaken down" until after at least two exercises.

Plan Structure

The DPP provides a basic outline for recovering data processing operations in the event of a disaster. Care has been taken to minimize the amount of duplicate information that must be recorded and maintained. Much of the information required for recovery is necessary for the normal operation of the Computer Operations Centers.

Recovery Process Overview

This section outlines the basic overall operation of the recovery process.

Operating Principle

The key Disaster Preparedness Plan (DPP) operating principle is flexibility. It is impossible to anticipate the exact nature of every emergency that may occur. It could be anything from a single disk crash to a relatively major system failure. It is the Recovery Manager's responsibility to communicate with City management and to determine, with City management, the severity of the problem and adjust the response accordingly.

Recovery Organization & Authority

The Recovery Manager is in charge of the disaster recovery effort. All Primary Recovery Team members report to the Recovery Manager. All other Recovery Team participants report to their assigned Primary Team member.

Disaster Declaration

A disaster as defined under this DPP shall be declared by the Recovery Manager as he or she deems appropriate

Plan Activation

The DPP shall be activated upon notification of the Primary Recovery Team personnel by the Recovery Manager.

Event Logging

This is an important task for the management of the disaster situation and the subsequent production of the summary report. The Event Log provides a definitive record of what has transpired. At first glance, event logging may seem like an inconvenient overhead task while there are more important disaster tasks to deal with. For any disaster situation that lasts more than a few hours, however, event logging is a valuable aid in the recovery effort. (see Appendix __)

An additional benefit of event logging is the historical record it provides for the production of the recovery report. Logging also provides a basis for reviewing the disaster plan after an exercise or real disaster to assist in making adjustments to the plan.

City Information

During a disaster recovery situation, there will be a requirement to notify the City and to keep City Management informed throughout the recovery process. All information inquires by the City should be handled by the Recovery Manager. The Recovery Manager and/or other appropriate staff will notify City management as needed. A management contact list can be found in Appendix ____.

The City will need to create the necessary manual procedures to support city business until the disaster has been recovered. These procedures can be anything from keeping documents that data was entered from, to logging all data entries manually in a specific log. The Information Technology Department will work with the City management to determine which manual procedures would be appropriate.

Network, Server, and Application Recovery List

Network

See APPENDIX __

Servers

See APPENDIX __

Applications

See APPENDIX __

Server Backup and Recovery Procedures

Server Backup Procedures

The City of Sunnyvale has over 100 servers of various operating systems, with current backup manually coordinated across numerous staff positions, backup tape units, and strategies. ArcServe 2000 is prevalent in the client server environment and is centrally operated using a console on the desktop of the Network Engineer.

THE NOVELL ENVIRONMENT

The Novell environment is used as the primary File and Print servers and host for the mail services. These servers are characterized by internal individual tape units using DLT tapes that are manually changed by the Network Engineer acting as system administrator. Backup software is centrally administered through ARCServe 2000 from a console on the desktop of the network engineer. Tape rotation is a separate tape for Monday, Tuesday, Wednesday, Thursday, Friday. The Friday tape is a full backup and Monday through Thursday incremental. No archive tape is created. Restores are handled primary from the Novell utility "Filer" to savage deleted files.

The backup window begins around 11:30 and takes a couple of hours. Campus backup takes 3+ hours.

Server: Nov1
NOS: Novell 5.1
Network segment 100 MBS NIC
Dell 2300 located in the Annex Basement
Disk size 22.6GB Free space 10GB
Primary Users: Information Technology and Finance file and print
Local DLT Tape

Server: Nov2
NOS: Novell 5.1
Network segment 100 MBS NIC
Dell 2400 located in the Annex Basement
Disk size 19.4GB Free space 12.7GB
Primary Users: Community Development, Office of the City Manager, Human Resources
print/file,(SIG,PSS?)
Local DLT Tape

Server: Nov3
NOS: Novell 5.1
Network segment 100 MBS NIC
Dell 2400 located in the Annex Basement

Disk size 19.4 Free space 5.45GB
Primary Users: Public Works, Library file and print
Local DLT Tape

Server: DPS
NOS: Novell 5.1
Network segment 100 MBS NIC
Dell 2300 located in the Annex Basement
Disk size 5.85GB Free space 0MB
Primary Users: Department of Public Safety headquarters and Fire Stations file and print
Local DAT Tape, Currently attempting to replace with DLT.

Server: Recware
NOS: Novell 5.1
Network segment 100 MBS NIC with T1 connectivity back to Server Room
Dell 2400 located at the Community Center
Tape rotation administered remotely by X
Backup administered centrally by System Administrator using Groupwise agent for mail post office.
Disk size Free space
Primary Users: GroupWise and Parks and Recreation file and print
Local DLT Tape

Server: CorpYard
NOS: Novell 4.x
Network segment 100 MBS NIC with T1 connectivity back to Server Room
Dell 2400 located at the Corp Yard
Tape rotation administered remotely by X
Backup administered centrally by System Administrator using Groupwise agent Disk size Free
space
Primary Users: Groupwise File and Print
Local DLT Tape

Server: WPCP
NOS: Novell 5.1
Network segment 100 MBS NIC with T1 connectivity back to Server Room
Dell 2400 located at the Water Pollution Control Plant
Tape rotation administered remotely by on-site personnel
Backup administered centrally by System Administrator using Groupwise agent Disk size Free
space
Primary Users: Groupwise Water Pollution Control Plant File and Print
Local DLT Tape

Server: Campus GPW-Groupwise Post Office
NOS: Novell 5.1
Network segment 100 MBS NIC

Dell 6300 located in the Annex Basement
Primary Users: Campus departments
Local DLT Tape

Server: Annex2, Engineering Drawings.
NOS: Novell 5.1
Network segment 100 MBS NIC
Dell 6300 located in the Annex Basement
Local DLT Tape

THE WINDOWS ENVIRONMENT

Microsoft Window server operating systems within the City of Sunnyvale consists of Windows NT and Windows 2000. These servers are used primarily for web services, application servers, application development and staging purposes. Since 1999, backup in the Windows environment (with a few exceptions) has been accomplished using an Exabyte Mammoth Tape Library. The transfer rate of the Mammoth Tape Drive is 10.8 GB per hour or 3 MB per second based on the compression rate of 2.5:1. The Library with a "media server" Benton, running ARCServe 2000 on a Dell 2400 using NT 4 SP 3 is located in the Annex Computer Room as are the servers being backed up by it.

The Exabyte Tape Library holds ten proprietary Mammoth 40GB compressed tapes (1/2 TB Storage) with robotic arm loading to a single read/write drive. The Library has been configured with two logical volumes. The first volume is used to backup weekly tapes and the second volume is used to backup incremental weekday dailies. The backup window is set at 6:20 pm Sunday and takes 5 to 6 hours.

The following servers and applications located in the City Hall Annex computer room are backed up using the Exabyte Tape Library.

Server: Eureka
NOS: Windows NT 4 SP 3
Application: Maximo
Developer Lead: Linda Lee
Directories and all subsequent subdirectories:
 D:\Changes_Doc
 D:\Gasboy
 D:\NDI
 D:\orant
 E:\PUBLICSHARE
 E:\screens
Retention: One week

Server: DPSWeb
NOS: Windows NT 4 SP 5
Application: MS IIS 4.x Intranet web server for Dept of Public Safety

Developer Lead: Helen Kwan

Directories and all subsequent subdirectories:

D:\inetpub\wwwroot

Retention: One week

Server: Angel

NOS: Windows NT 4

Application: Timesheet

Developer Lead: Al Jong

Directories and all subsequent subdirectories:

D:\timesheet

D:\WPCP

registry

Retention: One Week

Server: Jackson

NOS: Windows NT 4 SP 5

Application: SBT Accounting for SCI3

Developer Lead: Helen Kwan

Directories:

Retention:

Server: Honeywell

NOS: Windows NT 4 SP 5

Application: Honeywell Key Card Security System

Developer Lead: Helen Kwan

Directories: ips

Personfldr

postoffice

Retention:

Server: Jasmine

NOS: Windows NT 4 SP

Application: MS IIS 4.x Intranet Web server

Developer Lead: Helen Kwan

Directories and all subsequent subdirectories:

D:\inetpub

Retention: One Week

Server: Washington

NOS: Windows NT 4 SP 5

Application: Network Fax

Developer Lead: Helen Kwan

Directories: C:\

registry

Retention: One Week

The following application servers are currently backing up to local internal tape drives.

Server: TFP Mugshot

NOS: Windows NT

Application: Mugshot

Developer Lead: Lan Lee

Tape Operator: Rob Swift, DPS

Directories: C:\

registry

Retention: To be determined.

The following windows-based application servers are backed up on an "as-needed" basis as requested by the developer.

Server: Draweb

NOS: Windows NT 4 SP 5

Application: Library Web Server

Developer Lead: Helen Kwan

Directories:

Retention:

Server: Booker

NOS: Windows NT 4 SP 5

Application: Crystal Report Server

Developer Lead: Linda Lee

Directories:

THE IBM RS-6000 AIX ENVIRONMENT

The RS-6000 (AIX 4.0) houses the Computer Aided Dispatch and Records Management System applications for DPS.

The RS-6000 has two applications: CAD and RMS.

CAD is backed up using a seven day tape rotation (S/M/T/W/T/F/S), all holidays included. There is a Monday tape, a Tuesday tape, etc. and when the rotation hits Monday again, the Monday tape is overwritten. No tapes are held offsite. Tapes are held on an open shelf in the same room as the RS-6000. No archive tape is retained.

RMS is backed up using a four week business day tape rotation (M/T/W/T/F). There is a first Monday tape, a first Tuesday tape, etc. and when the rotation hits Monday again, the second Monday tape is

written. At the fifth week, the first Monday tape is overwritten. Friday data is backed up on Monday morning at 2 am. A separate End of Accounting Period tape is archived in a fireproof safe in City Hall. All other tapes are held on an open shelf in the same room as the RS-6000.

The backup job was setup by Tiberon Systems. Tiburon uses the Unix utility "mksysb" to make a bootable "system backup" to tape. The backup job is scheduled to run unattended but does not eject the tape cartridge so it will be overwritten if not manually changed.

THE HP 3000 MPEXI ENVIRONMENT

The HP 3000-947, Sunny8, (MPEXI) hosts the Financial System, Payroll, Purchasing and Business License applications.

Sunny8 is backed up on a Tuesday through Saturday (T/W/T/F/S) tape rotation with a Week 1 through Week 3 (W1/W2/W3) tape rotation for each Monday backup, and an End of Accounting Period (EOP) tape for Week 4. Tuesday through Friday tapes are recycled each week. Week 1 – 3 tapes are recycled each four weeks, and the End of Accounting Period is maintained onsite in a fire proof safe for 7 years.

Each Week tape is a full backup including system files. Tuesday through Saturday tapes are incremental on what has changed.

A separate Payroll tape is run manually at the completion of each payroll. The Payroll tape is maintained onsite in a fire proof safe for 8 years.

No tapes are held offsite.

The daily and weekly backup jobs were written by Bob Varesio and are scheduled to run unattended. The backup job documentation is attached in the Appendix. The backup job does not eject the tape but the Tape Unit goes "Out of ready status" when the backup is completed as an overwrite protection. The payroll backup job was written by Bob Varesio. A commercial product, Tapes3000 Management, stores tape label and content information in a database application.

Once a month, the tape drive is used as a supplemental disk while an Electronic Purchasing application is run. It uses a scratch tape and is not retained.

The HP 3000-957, Sunny3, (MPEXI) hosts the Library Application.

Sunny3 is backed up on a Monday through Friday tape rotation (M/T/W/T/F) with a Week 1 through Week 3 tape rotation (W1/W2/W3) for each Saturday backup, and an End of Accounting Period tape (EOP) for Week 4. Monday through Friday tapes are recycled each week. Week 1 – 3 tapes are recycled each four weeks, and the End of Accounting Period is maintained onsite in a fire proof safe for 7 years.

Each Week tape is a full backup including system files. Monday through Friday tapes are incremental on what has changed.

No tapes are held offsite.

The daily and weekly backup jobs were written by Bob Varesio and are scheduled to run unattended. The backup job is scheduled to run unattended but does not eject the tape cartridge so it will be overwritten if not manually changed. A commercial product, Tapes3000 Management, stores tape label and content information in a database application.

THE HP 9000 HP UX ENVIRONMENT

Taaffee, which houses the Performance Accounting System, is backed up to tape using scripts written by Bob Varesio of UNIX system commands (i.e. fbackup). The commands suspend the Oracle database and it is a full backup including system files. This backup is scheduled to run on Monday mornings around 1:30 am. There are no incremental or differentials backups run during the week. The weekly tape is on a six week rotation schedule. Bob Varesio is responsible for handling the tapes which are kept at Bob's desk and no copies are held off-site.

Francis, which houses the iProcurement system, is backed up to tape using UNIX commands by Bob Varesio on a demand basis. A back up strategy will be developed when this application comes online into production.

Sunny 6, which houses the older KPMG Financial System, is no longer in production and backed up using UNIX commands by Bob Varesio on an as-needed basis.

THE AS-400 ENVIRONMENT

The AS-400 houses the HTE Utility Billing Application.

The AS-400 is backed up on a Tuesday through Friday (T/W/T/F) tape rotation with a Week 1 through Week 3 tape rotation (W1/W2/W3) for each Saturday backup, and an End of Accounting Period tape for Week 4. Tuesday through Friday tapes are recycled each week. Week 1 – 3 tapes are recycled each four weeks, and the End of Accounting Period is maintained onsite in a fire proof safe for 7 years. There is no backup on Monday since the system is not used on Sunday.

A separate tape is created at End of Accounting Period that holds the print spool files. These are maintained onsite in a fire proof safe for 4 years.

Each Week tape is a full backup including system files. Tuesday through Friday tapes are incremental on what has changed.

No tapes are held offsite.

The daily and weekly backup jobs were written by HTE and are scheduled to run unattended. The backup job documentation is attached in the Appendix. The tapes eject after completion and require manual intervention to change the tapes.

The new AS/400 270 has a seven tape LTO library attached as well as recycling the current 8 MM tape unit. Each LTO tape holds 100 GB (200 GB compressed). The software will include BRMS (Backup & Recovery Media Services) which will simplify scheduling and tracking backup jobs.

Server Recovery Procedures

The Network Engineer or the Programmer in charge of the application server will arrange to have the most recent version of the backup files on site for recovery of any Servers listed in APPENDIX ____.

Recovery Procedures

1. In the event of a disaster the IT Manager will assume the responsibilities of the Administrator of the Disaster Recovery plan. Contact information can be found in Contact List (see Appendix ____)
2. Begin documentation of the problems using Event Log (see Appendix ____).
3. Verify that the latest copy of the backup for the problem server is available. In the case of a server this will be the previous night's backup tape.
4. Contact the appropriate vendor or vendors immediately (see APPENDICES B). This is extremely important because the service agreements with hardware and software vendors have response times levels based on the original notification of a problem. At this early stage you may not have determined the exact cause of the problem, it may be a good practice to notify all of the hardware and software vendors that might be needed to assist in the recovery.
5. Establish timeline for progress updates with customer. At a minimum the customer should be given a progress report on an hourly basis.
6. Continue problem determination. No direct action should be taken to resolve the problem until the Disaster recovery manager and/or the Director of Information Technology Department have reviewed the options and agree on the recovery plan.
7. The recovery activity will not begin until there is agreement on the definition of the problem and the recovery plan.

Hardware Recovery

Depending upon the system involved, the primary hardware technician required for recovery will vary. It might include the Network Engineer for a system resource, a programmer for an application server, or a vendor technician for major systems under service contract.

1. If the hardware technician is not onsite at this time contact the hardware vendor to determine status of their technician. The vendor is required to have a technician onsite within the time frame specific in our maintenance contract. This information can be found in Vendor Contact (see APPENDIX ____).
2. When the hardware problem has been corrected reboot the device to see if service has been restored. If not continue to work with the hardware technician to determine if the problem is still hardware or software.

3. If the problem appears to be hardware continue to work with the vendor until the problem is resolved. Be sure to escalate the problem to the next highest level within the vendor organization if the problem is not resolved in a timely manner.
4. When the hardware problem is fixed reboot the system to see if services are restored. If the problem has been corrected, notify the City representative that services have been restored. Close out the Event Log and begin a post Event report.
5. It may be necessary to restore software or data files after a hardware failure. If it is determined that this is necessary then follow the steps outlined in SOFTWARE RECOVERY PROCEDURES.

Software Recovery Procedure

1. No data or application files will be deleted unless the Disaster Recovery manager and the programmer responsible for the application agree to this action as part of the recovery process.
2. Before restoration of any vendor software application or data files be sure to contact the software vendors' Help Desk or Technical Support Group. Additional help may be found on the vendor's WEB site under Frequently Asked Questions (FAQ).
3. Earlier in the event a problem ticket should have been opened with this vendor. Before any recovery activity begins be sure to contact the vendors' help organization to verify that the recovery plan is correct.
4. Execute plan
5. Continue to work with vendors' help desk or City of Sunnyvale programmer until problem is resolved.
6. Maintain the Event Log and provide progress reports as scheduled.
7. When the problem has been corrected, reboot the system and verify that services are fully restored. Notify the Director of Information Technology and/or City contact of the status. Close out Event Log and begin a Post Event Report.

Network Backup and Recovery Procedures

Network Backup Procedures

The "Network" consists of the DNS server, the Checkpoint Firewall, the Cabletron Hubs and MMAC8s and the Cisco Routers and Switches. The Annex Computer room at City Hall contains the Primary DNS server, the Checkpoint firewall and a primary hub for the city's FDDI Ring. The DPS Computer Operations Center houses the Cisco 7500 connectivity for the WAN and Internet.

Documentation Procedures

- It is not necessary to create daily backups of the network configuration files.
- Each time a change is made to the configuration file for any network device a copy of the new configuration file is saved on \\CAMPUS\VOL1\ITUSERS\rtreanor\NETWORK\Router Logs. Hard copies of the configuration files are maintained in the file cabinet in the Network Engineer's area.

Hardware Availability

The Information Technology Department maintains a spare of most critical network equipment. In a disaster, damaged equipment would be replaced from inventory, relocated from less critical city locations, or loaned/purchased from appropriate vendors. See Appendix __ for a list of vendors.

Network Recovery Procedures

The Network Engineer will arrange to have the most recent version of the backup files or hard copies on site to aide in the recovery of Network functions.

Recovery Procedures

1. In the event of a disaster the Technical Support Manger will assume the responsibilities of the Administrator of the disaster recovery plan. Contact information can be found in Contact List (see Appendix __)
2. Begin documentation of the problems using Event Log (see Appendix __).
3. Verify that the latest copy of the backup for the problem device is available. In the case of the network this would be a copy of the last configuration floppy, printout of the latest configuration or one of the copies of configuration information located in the network documentation
4. Contact the appropriate vendor or vendors immediately (see APPENDIX __). This is extremely important because the service agreements with hardware and software vendors have response times levels based on the original notification of a problem. At this early stage you may not have determined the exact cause of the problem, it maybe a good practice to notify all of the hardware and software vendors that might be needed to assist in the recovery.
5. Establish timeline for progress updates with City representative. At a minimum the City Representative should be given a progress report on an hourly basis.
6. Continue problem determination. No direct action should be taken to resolve the problem until the Disaster recovery manager and/or the City representative have reviewed the options and agree on the recovery plan.
7. The recovery activity will not begin until there is agreement on the definition of the problem and the recovery plan.

Hardware Recovery

1. If the hardware technician is not onsite at this time, contact the hardware vendor to determine status of their technician. The vendor is required to have a technician onsite within the time frame specific in our maintenance contract. This information can be found in Vendor Contact (see APPENDIX __).
2. When the hardware problem has been corrected, reboot the device to see if service has been restored.. If not continue to work with the hardware technician to determine if the problem is hardware or software.
3. If the problem appears to be hardware continue to work with the vendor until the problem is resolved. Be sure to escalate the problem to the next highest level within the vendor organization if the problem is not resolved in a timely manner.

4. When the hardware problem is fixed reboot the system to verify that services are restored. If the problem has been corrected, notify the City representative that services have been restored. Close out the Event Log and begin a post Event report.
5. It maybe necessary to restore software or data files after a hardware failure. If it is determined that this is necessary then follow the steps outlined in SOFTWARE RECOVERY PROCEDURES.

Software Recovery Procedure

1. No data or application files will be deleted unless the Disaster Recovery manager and/or the Director of Information Technology or his designate agree to this action as part of the recovery process.
2. Before restoration of any software application or data files be sure to contact the software vendors' Help Desk or Technical Support Group. Additional help maybe found on the vendor's WEB site under Frequently Asked Questions (FAQ).
3. Earlier in the event a problem ticket should have been opened with this vendor. Before any recovery activity begins be sure to contact the vendors' help organization to verify that the recovery plan is correct.
4. Execute plan
5. Continue to work with vendors' help desk until problem is resolved.
6. Maintain the Event Log and provide progress reports as scheduled.
7. When the problem has been corrected, reboot the system and verify that services are fully restored. Notify the City representative of the status. Close out Event Log and begin a Post Event Report.

Accounting and Revenue Recovery

Revenue is responsible for recovery procedures of their day-to-day operational office environment. Their recovery consists of manual procedures as identified by city management that would allow the client to recover the following: Cashiering, Utility Billing, Service Orders and Meter readings.

Accounting is responsible for recovery procedures of their day-to-day operational office environment. The recovery consists of manual procedures as identified by city management that would allow them to recover the following: Payroll Checks, Direct Deposit Payroll, Tax Deposits, Accounts Payable, Accounts Receivable, Inventory, Purchasing.

Primary Recovery Team Assignments

The following pages list the Primary Recovery Team assignments for the execution of the DRP. All other ITD and City employees normally assigned to support data processing will support the Primary Recovery Team members as assigned during a disaster recovery operation.

Recovery Manager

The Recovery Manager has overall responsibility for managing the disaster and the response. All members of the Disaster Recovery Team ultimately report to the Recovery Manager. It is the Recovery Manager's responsibility to confer with the City Finance Director and City Administrative Office and others as appropriate to keep them informed of the disaster and recovery status.

Director of Information Technology	Name Shawn Hernandez	See Contact List Appendix ____
IT Services Manager	Name Marilyn Crane	See Contact List Appendix ____
Application Support Manager	Name Cheryl Bunnell	See contact List Appendix ____

Recovery Manager Assignments

- Determine that a disaster has occurred and that the Disaster Preparedness Plan must be activated.
- Notify the City Finance Director, and other City departments and staff as appropriate.
- Document the date, time, and circumstances requiring the disaster declaration.
- Call for a disaster preparedness meeting with all parties affected, City and ITD staff.
- Determine the extent of the damage or outage.
- Determine the appropriate recovery response.
- Make the specific task assignments required for the particular disaster circumstances.

- Set the time for the next Disaster Recovery Meeting.
- Modify the assignments and response as deemed necessary.
- Keep the City Finance Director informed of the situation.
- Determine when the recovery effort is concluded and notify the appropriate City staff.
- Complete a Disaster Recovery Event and Disbursement Log form and distribute as appropriate.

ITD Operations Recovery Team

The Operations Recovery Team has the key role in recovering operations.

Technical Support Manager	Name Marilyn Crane	See Contact List Appendix ____	
Network Engineers	Names Mike Papa Mike Dreelan	See Contact List Appendix ____	
Operations	Name Clarín Paap		
Programmers	Name As appropriate	See Contact List Appendix ____	
Department Application Leads	Name As appropriate	See Contact List Appendix ____	

Finance Operations Recovery Team

Finance	Name Mary Bradley	See Contact List Appendix ____	
	Name Finance Manager	See Contact List Appendix ____	
	Name Grace Kim	See Contact List Appendix ____	
	Name Tim Kirby	See Contact List Appendix ____	
	Name Terese Balbo	See Contact List Appendix ____	

Operations Team Assignments

- Provide an accurate assessment of the operations damage and situation.
- Provide an accurate assessment of the critical processing tasks to be accomplished and their priorities.
- Determine which normal processes that can be suspended during the recovery effort.
- Recommend appropriate recovery actions.
- Prioritize and assign recovery tasks to appropriate personnel.
- Handle contact with all vendors required to support operations recovery.
- Coordinate all activities relating to operations recovery and critical application processing.
- Determine and prioritize the emergency programming changes necessary to support emergency operations.
- Assign applications personnel to make emergency programming changes to support operations recovery.
- Ensure the necessary programming changes are accomplished quickly and accurately.
- Keep the Recovery Manager informed of the operations recovery status.

Department of Public Safety

The Department of Public Safety provides vital services to the public on a daily basis. It is critical that the manual procedures used during a disaster still provide the public with public safety effectively. Public Safety staff play an important role in providing these services and in recovery of the system. It is important to notify designated City staff timely so that they may prepare for the recovery.

Public Safety Primary	Name Chief of Public Safety	See Contact List Appendix ____	
Public Safety Secondary	Name Technical Services Bureau Manager	See Contact List Appendix ____	
ITD Technical Services	Name Marilyn Crane	See Contact List Appendix ____	
ITD Programmer	Name Lan Le	See Contact List Appendix ____	

Department of Public Safety Assignments

- Determine with ITD approximate time the system will be available. Notify appropriate city management staff.
- Review manual procedures for handling business during a disaster outage.
- Assemble city staff required to perform manual disaster procedures. Go over procedures and assignments with staff.
- Coordinate issues with ITD..
- Document steps taken through the recovery process. Review manual disaster recovery procedures and update as appropriate
- Keep the Recovery Manager and Operations Team informed of the network status.

Appendices A

Disaster Recovery Event and Disbursement Log

The Recovery Event and Disbursement Report should be filled out every time the Disaster Preparedness Document is used in a recovery process. If equipment is replaced update the City equipment inventory list. To be reviewed by the Recovery Manager.

Date _____ Time _____

Logged By _____ Location _____

Date of Disaster _____ Time of Disaster _____

System Affected _____ System Affected _____ System Affected _____

Disaster Description

Damage Assessment - Identify all equipment being replaced (use additional pages as needed)

Equipment Type Old: _____ Serial # _____ Model # _____

Replaced Equipment (use additional pages as needed)

Equipment Type New: _____ Serial # _____ Model # _____

Damage Estimated Replacement Cost:

Computer Services Recommendation:

Action Taken: _____

City Approval (if required for ordering replacement equipment)

Signature: _____

Date : _____ Time: _____

Event Log

[illegible]

Appendix

Contact List

For details on the Emergency contact list see: